



Meg – Hacker Tools: Endpoint scan the masses! ☐☐

BY ANNA HAMMOND · FEBRUARY 1, 2022 · LAST UPDATED ON AUGUST 8, 2026

 **Want to read the latest version? Visit the link below:**

<https://www.intigriti.com/researchers/blog/hacking-tools/hacker-tools-meg>

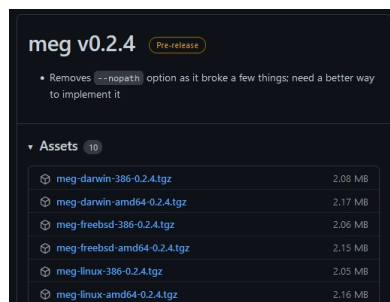
You've just enumerated all the subdomains of your target and what? There's 400 of them? Are you going to start individual scans to find endpoints on them? No you're not! You're going to use Meg, of course!

☐☐ What is Meg?

Meg is not the girl nextdoor, no it's an amazing tool you need to know about! As more and more people get into bug bounty, more and more scans are being launched and some servers are just not ready for them. We want to scan a ton of endpoints, but we want the server to stay responsive, so that we can continue scanning.

Tomnomnom has come up with the brilliant idea of not just scanning our targets one-by-one, but distributing traffic between them. Instead of barraging a single target with 100 requests per second, we send 1 request to 100 targets per second. This way, everyone can keep up and we still receive the same amount of results!

☐☐ Installing Meg



Installing Meg couldn't be easier! Just follow these steps

- Go to the [releases page](#) on GitHub
- Download the binary for your architecture
- Run `tar -zxvf binary.tgz` to extract it
- Enjoy!

Our first run!

Let's get into it! Let's finally start using Meg!

The things you need in order to run Meg are:

- A wordlist of endpoints you want to scan. [SecLists](#) is a great place to get started.
- A list of targets to scan. In this case, I'll take some intigrity subdomains, however you will probably want to take the output from another discovery tool!

Now we're really ready to go! I'll run `meg --verbose wordlist hosts.txt` Note that I'm using the `--verbose` flag here just to make what the tool is doing visible. This is of course not needed. Let's assess the command line output of the tool!

```
(PinkDraconian@intigrity) [~/Documents/HackerTools/Meg]
$ /opt/meg/meg --verbose /usr/share/dirb/wordlists/big.txt hosts.txt
out/challenge.intigrity.io/8cdeb6f152a06206aa431178fba9ede0f9e0706 http://challenge.intigrity.io/images (308 Permanent Redirect)
out/intigrity.com/baa5b496c8ee7def478620309f8f96025a1e174a https://intigrity.com/! (301 Moved Permanently)
out/blog.intigrity.com/c4cb6826075d7b4613e5725d432e4c024b33ff34 https://blog.intigrity.com/!_images (404 Not Found)
out/go.intigrity.com/6d42ade4f3472f480c7088b1b08fde96724ec5b0 http://go.intigrity.com/!_images (302 Found)
out/challenge.intigrity.io/00b2c4c4d8f4d7047ced2a8094a3f5e1246b09 http://challenge.intigrity.io/! (308 Permanent Redirect)
out/intigrity.com/a90931c59def70c535c520f23bde053c2df72bf https://intigrity.com/!_archives (301 Moved Permanently)
out/blog.intigrity.com/21fea5293cce87470bb4f5f9241b3881d2a5d86c https://blog.intigrity.com/! (301 Moved Permanently)
out/go.intigrity.com/1e0df7e9fee40e92dfc1138c1a252cccd437cfac http://go.intigrity.com/! (302 Found)
out/challenge.intigrity.io/8cf4ac85b1c1a2b121d98ec08f8eba1919097ae http://challenge.intigrity.io/!_images (308 Permanent Redirect)
out/intigrity.com/0b84edaba5824cd3933c86c71f8d2c0bd8254975 https://intigrity.com/!_images (301 Moved Permanently)
out/go.intigrity.com/e049580198e74707c4eb77418031269db6173b8 http://go.intigrity.com/!_backup (302 Found)
out/blog.intigrity.com/df3e3b10339b1a422aea61b2e1e959f3f182ff6 https://blog.intigrity.com/!_backup (404 Not Found)
out/challenge.intigrity.io/06d23c7ee066e7a6e30570374257524a5e86a6b1 http://challenge.intigrity.io/!_backup (308 Permanent Redirect)
out/intigrity.com/bf3f5f24e7fe948b84e240faf0d86424ebf8728d https://intigrity.com/!_backup (301 Moved Permanently)
out/go.intigrity.com/2385b077f63be2c5d6c2988904f462805dd444c9 https://go.intigrity.com/!_archives (302 Found)
out/blog.intigrity.com/dbea36a2dc5e866c8ccfd3b2c818947a7183bee2 https://blog.intigrity.com/!_archives (404 Not Found)
out/challenge.intigrity.io/397cb0ec59be2f7b0765bb2598d127b11f343a7 http://challenge.intigrity.io/!_archives (308 Permanent Redirect)
out/intigrity.com/d83883a5b76ad81b9972b119c406a63200bf25a https://intigrity.com/!_images (301 Moved Permanently)
out/blog.intigrity.com/988be930f4d879ad937dc585191718bee96cadb https://blog.intigrity.com/!_images (404 Not Found)
out/go.intigrity.com/619edef9890cf333ae56da58937ca03cc0213ca https://go.intigrity.com/!_images (302 Found)
out/challenge.intigrity.io/9674e7c561e2563e580341e424a6c091b668069 http://challenge.intigrity.io/!_res (308 Permanent Redirect)
```

Meg output

The output here shows the location where it has stored the result of the request, then the endpoint and then the status code. We can see here how it sends the same request to each endpoint and gathers its response. This is how the load for the server is greatly decreased!

Now, without the `--verbose` option, the tool doesn't print out this information, but it saves it to `out/index` (output directory can be changed). From there you can simply use `grep` to get all the results for specific targets as shown here

```
(PinkDraconian@intigrity) [~/Documents/HackerTools/Meg/out]
$ cat index | grep blog.intigrity.com
out/blog.intigrity.com/3f4ffae7853c48993287e1a31037ca8fb3fc0eb2 https://blog.intigrity.com/! (301 Moved Permanently)
out/blog.intigrity.com/c4cb6826075d7b4613e5725d432e4c024b33ff34 https://blog.intigrity.com/!_images (404 Not Found)
out/blog.intigrity.com/21fea5293cce87470bb4f5f9241b3881d2a5d86c https://blog.intigrity.com/! (301 Moved Permanently)
out/blog.intigrity.com/df3e3b10339b1a422aea61b2e1e959f3f182ff6 https://blog.intigrity.com/!_backup (404 Not Found)
out/blog.intigrity.com/dbea36a2dc5e866c8ccfd3b2c818947a7183bee2 https://blog.intigrity.com/!_archives (404 Not Found)
out/blog.intigrity.com/988be930f4d879ad937dc585191718bee96cadb https://blog.intigrity.com/!_images (404 Not Found)
out/blog.intigrity.com/d24bb33ffdd99e44cf5dcea7a2a9ed91f19b911 https://blog.intigrity.com/!_res (404 Not Found)
out/blog.intigrity.com/c27cbe0f539ae0940ccebcbf48a5c135369bc97ce https://blog.intigrity.com/!_textove_diskuse (404 Not Found)
out/blog.intigrity.com/140d20694c7ec43e5b09b1bf898a7d3867f9e98 https://blog.intigrity.com/!_ut (404 Not Found)
out/blog.intigrity.com/bb43044e0d6a6afe41538f854fc1a2468398ab90 https://blog.intigrity.com/!_bash_history (403 Forbidden)
out/blog.intigrity.com/057c6c4d405e4b30338d8606eb0432d26cbc8a8c https://blog.intigrity.com/!_bashrc (403 Forbidden)
out/blog.intigrity.com/e18a9d804f9fa657f4cc93146451b7d41cd12126 https://blog.intigrity.com/!_cvs (403 Forbidden)
out/blog.intigrity.com/9bf3242ea5f9db5ce90f9a4f3966f7c1837aaaa1 https://blog.intigrity.com/!_cvsignore (403 Forbidden)
out/blog.intigrity.com/2c854c395202c325a8082844f02516b0709492e4 https://blog.intigrity.com/!_forward (403 Forbidden)
out/blog.intigrity.com/c6642c4d4b1164a795735a315376842d5f95610a https://blog.intigrity.com/!_history (403 Forbidden)
out/blog.intigrity.com/a4271e8f56c0cc9be91fcaa42504015f07785364 https://blog.intigrity.com/!_htaccess (403 Forbidden)
out/blog.intigrity.com/d368597006e0e277e3998e254b87f53eb5784890 https://blog.intigrity.com/!_httppasswd (403 Forbidden)
out/blog.intigrity.com/2ab9c19f687d735a75b032d468bbbc420da514e6 https://blog.intigrity.com/!_listing (403 Forbidden)
out/blog.intigrity.com/3c2b7a723c745634837f6d57dcd8800703b1cf96 https://blog.intigrity.com/!_passwd (403 Forbidden)
out/blog.intigrity.com/b04f573b9b052cf304fc17a36563305505c8e767 https://blog.intigrity.com/!_perf (403 Forbidden)
```

Meg index grepping

You can also see the responses for these requests by just looking in the files for them, an example of which is shown below

```
(PinkDraconian@intigriti)-[~/Documents/HackerTools/Meg]
$ cat out/blog.intigriti.com/b04f573b9b052cf304fc17a36563305505c8e767
https://blog.intigriti.com/.perf

> GET /.perf HTTP/1.1
> Host: blog.intigriti.com
> User-Agent: Mozilla/5.0 (compatible; meg/0.2; +https://github.com/tomnomnom/meg)

< HTTP/1.1 403 Forbidden
< Content-Length: 146
< Strict-Transport-Security: max-age=31536000
< X-Ac: 1.ams_atomic_ams
< Server: nginx
< Date: Wed, 26 Jan 2022 10:00:39 GMT
< Content-Type: text/html

<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Meg showing output file

Features

You may have seen some things you don't really fancy in the results shown before. Perhaps you only want to capture 200 OK responses or you want to send HEAD requests instead of GET requests. All of that is of course possible. Let's discuss Meg's `--help` page!

```
(PinkDraconian@intigriti)-[~/Documents/HackerTools/Meg]
$ /opt/meg/meg --help
Request many paths for many hosts

Usage:
  meg [path|pathsFile] [hostsFile] [outputDir]

Options:
  -c, --concurrency <val>    Set the concurrency level (default: 20)
  -d, --delay <millis>        Milliseconds between requests to the same host (default: 5000)
  -H, --header <header>       Send a custom HTTP header
  -L, --location               Follow redirects / location header
  -r, --rawhttp                Use the rawhttp library for requests (experimental)
  -s, --savestatus <status>    Save only responses with specific status code
  -t, --timeout <millis>      Set the HTTP timeout (default: 10000)
  -v, --verbose                Verbose mode
  -X, --method <method>       HTTP method (default: GET)

Defaults:
  pathsFile: ./paths
  hostsFile: ./hosts
  outputDir: ./out

Paths file format:
  /robots.txt
  /package.json
  /security.txt

Hosts file format:
  http://example.com
  https://example.edu
  https://example.net

Examples:
  meg /robots.txt
  meg paths.txt hosts.txt output
```

Meg `--help`

- `-c` or `--concurrency` : This option can be used to change the concurrency level. Higher numbers here mean more requests being sent out at once.
- `-d` or `--delay` : This option relates to the delay between every request to the same host in milliseconds. This tool is made to be slower to the server, however, in certain configurations, it can still be too fast. Luckily the default here is already 5 seconds.

- `-H` or `--header` : Need to set a specific header for each request, worry no more and set this option!
- `-L` or `--location` : Getting a lot of 302's? Use this option to follow those redirects!
- `-s` or `--savestatus` : Only save responses with specific status codes.
- `-t` or `--timeout` : Failing requests will timeout after this amount of milliseconds. The default is 10000.
- `-v` or `--verbose` : If you need some more output, then this option is for you!
- `-X` or `--method` : Change the request method from GET to for example HEAD. I highly recommend playing around with sending HEAD requests!

Conclusion

Meg is a simple, yet helpful tool designed to help you get more efficient and to go easier on your targets! Start using it today to hack even more efficiently!

If you would like to recommend a tool for us to cover next week, then be sure to let us know down below. Also be sure to check out [all the previous Hacker Tools articles](#), such as [the last one on EyeWitness](#).

Did you know that there is a video accompanying this article? Check out [the playlist](#)!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com